10 years of DNSSEC: what, how and most importantly, why?

For many people, Internet security is about anti-virus software, firewalls and regularly changing passwords. However, at .eu we have a wider view on how to protect our 3.6 million .eu domain names.

The behind-the-scenes security measure that .eu implemented exactly a decade ago is called DNSSEC - short for Domain Name System Security Extensions. It gives online consumers greater confidence by reducing the chance that they will be led to fake websites and tricked into supplying personal information.

What is DNSSEC?

The basis of any Internet presence is a domain name, such as ‘eurid.eu’, which is used for websites and emails. Looking up a domain name, or URL, involves a a browser issuing a request to find the website it is looking for.

With DNSSEC, name servers and browsers can verify and authenticate the answers they receive. This means that there is a smaller chance that Internet users can be redirected to ill-intentioned websites or have their email intercepted by rogue systems.

How does it work?

DNSSEC works by checking answers at each level of Internet infrastructure – the Domain Name System

(DNS) – where each level in the hierarchy verifies the level above through what is known as a ‘chain of trust’.

.eu implemented DNSSEC in September 2010 and was one of the first of the world’s largest top-level domains to have a complete DNSSEC chain of trust. Since then, 16 % of .eu registrations have been signed with DNSSEC.

Why is DNSSEC important?

The major benefit of DNSSEC is that it gives authenticity and integrity to DNS replies by building security into the fabric of the Internet. Without this security protocol, attackers can position themselves next to genuine DNS servers and launch so-called cache-poisoning attacks by supplying false data, and so redirecting traffic.

A more tangible benefit of DNSSEC is that it can prevent website owners from losing valuable traffic to their websites.

If a potential customer types a web address into their browser, but makes a spelling mistake, they should normally get an error page saying that the domain does not exist, which tells them that the address they typed was incorrect. However, if the website is not protected by DNSSEC, there is a chance that the answer to their browser’s DNS request is modified to return an answer which could redirect them to a third-party webpage. This website will present a list of alternatives, which may not include the website they were originally looking for.

Protecting your website with DNSSEC ensures that your customers will see a DNS error page if they misspell your URL. This means that they will type it again and successfully reach their desired destination - your website.

What can I do?

DNSSEC helps make the Internet safer. As more top-level domains implement DNSSEC, it is gaining momentum and becoming more commonplace. But more work is needed so that everyone with a .eu domain name, website or email address can benefit from the collective online security that DNSSEC offers.

Please instruct your domain name provider- your registrar - to add DNSSEC to your .eu domain name – a process known as signing – so that it joins the chain of trust and protects visitors to your website.

Even if you think you are protected online, you can always do more to minimise risk and stay one step ahead. As the cliché goes, it is always better to be safe than sorry.